Instituto Tecnológico de Cancún

Materia:

Fundamentos de Telecomunicaciones

Tarea:

Investigar sobre SIEM

Alumno: **Aguilar Moreno Jorge Axel**

Docente: **Ismael Jiménez Sánchez**

Horario: **17:00 – 18:00**

Ing. **Sistemas Computacionales**

5.-Semestre

SIEM

(Security Information and Events Management)

Gestión de Eventos e Información de Seguridad o SIEM por sus abreviaciones en el lenguaje original ***(Security Information and Events Management)*** es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas.

Objetivo

Como se mencione anteriormente su objetivo principal es poder **responder con rapidez y precisión ante las amenazas**. Tratan de visibilizar los ataques o las tendencias de ataque **en tiempo real** mediante la recopilación y el análisis de mensajes ordinarios, notificaciones de alarma y archivos de registros.

Ejemplos:

- Cortafuegos (Software y hardware)
- Interruptores
- Routers
- Servidores (Servidores de archivos, Servidores FTP, Servidores VPN, Servidores Proxy)
- Sistemas de IDS e IPS

Ventajas del SIEM

- **R**educe el mínimo de los perjuicios ocasionados.
- **T**odos los eventos de seguridad se documentan y archivan automáticamente a prueba de manipulaciones**.**
- **A**yuda a optimizar los recursos humanos.